Woodloes
Primary School

COMMUNITY
ACADEMIES TRUST

Online Safety Policy

Prepared by:	David Link Sarah Evans		Sept 2015
Ratified:	Sue Robinson		Oct 2015
Reviewed:	Sarah Burnard		Sept 2016
Reviewed:	Sue Robinson Sarah Burnard Mick Potter		Dec 2017

CONTENTS

Introduction

“The internet and related technologies are powerful tools, which open up new prospects for communication and collaboration. Education is embracing these new technologies as they bring with them fresh opportunities for both teachers and learners. To use these technologies effectively requires an awareness of the benefits and risks, the development of new skills, and an understanding of their appropriate and effective use both in and outside of the classroom”

Online Safety encompasses not only internet technologies but also electronic communications such as mobile phones and wireless technology (See Mobile Devices Policy). It highlights the need to educate children, young people and adults about the benefits, risks and responsibilities of using information technology and provides safeguards and awareness for users to enable them to control their online experiences.

The purpose of internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school’s management information and administration systems.

Internet use is part of the statutory National Curriculum and a necessary tool for learning. It is an essential element for education, business and social interaction. Access to the internet is therefore an entitlement for pupils who show a responsible and mature approach to its use. Our school has a duty to provide pupils with quality internet access.

Pupils will use the school’s Virtual Learning Environment (VLE) as a secure online learning platform both in school and at home. They are taught that for this platform, https signifies a secure, encrypted site, where information is shared safely within school.

Pupils use the internet outside school and need to learn how to evaluate online information and to take care of their own safety and security.

Some of the material on the internet is published for an adult audience and is unsuitable for children and young people. It is important that children and young people are made aware of appropriate behaviour in relation to contacting others and they must also understand that publishing personal information could compromise their security.

Writing and reviewing the Online Safety Policy

The Online Safety Policy has strong links with the Computing Curriculum and Safeguarding policies which are reviewed annually, as well as the Acceptable Use Agreement. The process of writing and reviewing will:

- Be completed by the school's appointed Online Safety Coordinator; the Online Safety Committee have an input into the content
- Be agreed by the Senior Management Team and approved by Governors

Aims and Objectives

The aim of the Online Safety Policy is to promote safe and appropriate practice through the establishment of clear and robust acceptable-use guidelines. The policy will:

- Provide staff with the key information to deal with online safety issues in a safe and effective manner
- Ensure that staff have the ability to deal with content, contact and conduct issues online
- Provide staff with a point of reference when dealing with online safety issues

Teaching and Learning

Online safety should be a focus in all areas of the curriculum and staff reinforce online safety messages in the use of computing across the curriculum.

- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- Where pupils are allowed to freely search the internet as part of a lesson, e.g. using search engines on PCs or iPads, staff must be vigilant in monitoring the content of the websites that are accessed as a result of these searches
- It is accepted that from time to time, for educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Network Manager (ICT Development Service / ICTDS) temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need
- Pupils are taught in all lessons to be critically aware of the content they access online and are guided to validate the accuracy of information (In relation to Online Safety curriculum overview)
- Pupils are taught to acknowledge the source of information used and respect copyright when using material accessed on the internet
- Email, online history and VLE communications are monitored
- Users must immediately report, to the Designated Safeguarding Lead (DSL) – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such communication
- Any digital communication between staff and pupils or parents / carers (email, chat, VLE etc.) must be professional in tone and content. These communications may only take place on official (monitored) school systems.

Personal email addresses, text messaging or public chat / social networking programmes must not be used for these communications

- Pupils are taught about email and online communication safety issues, such as the risks attached to the use of personal details. They are also taught strategies to deal with inappropriate content and are reminded of the need to communicate clearly and appropriately

Organisation

Pupils are taught how to evaluate internet content:

- If staff or pupils discover unsuitable sites, the URL, time, date and content must be reported to the Online Safety Coordinator who will then report it to Warwickshire ICT Development Service
- The school will ensure that the use of internet derived materials by staff and by pupils complies with copyright law
- Pupils are taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy

Authorised Internet Access:

- The school maintains a record of all staff and pupils who are granted internet access; this is reviewed and updated annually or when new staff are employed
- All staff are required to read and sign the Acceptable Use Agreement before using any school ICT resource. In addition, all parents and pupils are required to read and sign the Acceptable Use Agreement when the child starts school. The Acceptable Use Agreement is a cyclical review linked with pupils' start point and new reception entry

Managing Internet Access and filtering:

- The ICTDS team use Smoothwall's filtering system for all devices in Woodloes School, by using wireless authentication to connect users to their secure BYOND Network. The filtering system is sometimes referred to as the Warwickshire School's Gateway
- Virus protection is installed and updated regularly
- Security of the school information systems is reviewed regularly by the ICTD
- The Online Safety Co-ordinator and IT School Support Technician meet regularly to ensure filtering systems are in place and up to date
- The school uses the Warwickshire Broadband with its firewall and filters
- The school provides an additional level of protection through its deployment of Policy Central in partnership with Warwickshire ICTDS. This software monitors text appearing on the screen and keyboard input, identifying the use of words that are included on a list of 'banned words'. The software captures the screen, identifying machine and user details so appropriate action can be taken

Use of e-mail:

The school is provided with a login, password and email account for each pupil on entry to Woodloes School. Woodloes School do not currently use the email account, which is linked to Warwickshire's 365 learning platform, and do not provide pupils with the email address. Pupils are encouraged to communicate with teachers and pupils via the discussion groups and messaging services on the VLE. (Refer to the Computing Policy for VLE information.)

Published content and the school web site

- The contact details on the school's website should be the school address, e-mail and telephone number. Staff or pupil's personal information will not be published
- Staff will be allocated time to update the website and VLE regularly and these updates, such as class information pages, newsletters and photographs are reviewed by the Online Safety Co-ordinator and Head Teacher

Publishing pupils' images:

- Photographs that include pupils will be selected carefully and will not enable individual pupils to be identified by name (teachers are aware of pupils that should not be photographed for publication purposes)
- Written permission from parents or carers is obtained annually before photos of pupils are used for any purpose relating to the school

Social networking and personal publishing:

- Social networking sites, chat rooms and newsgroups are blocked on school devices by ICTDS
- Pupils and parents are taught never to reveal personal details of any kind which may identify them, their location or peers. Examples would include real name, address, mobile or landline phone numbers, school, IM address, e-mail address, names of friends, specific interests and clubs etc.
- Pupils and parents are advised not to place personal photos on social networking sites, particularly displaying the school logo on bags and jumpers as this is revealing person details
- Pupils and parents are advised on security settings and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Pupils are encouraged to invite only known friends and deny access and report other 'friend' invitations
- Pupils and parents are advised in the newsletter that the use of social network spaces outside school may be inappropriate for pupils
- Biannual online safety information meetings for parents and pupils are held in school

Protecting personal data:

- Personal data is recorded, processed, transferred and made available according to the Data Protection Act 1998
- Personal data should only be used on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which personal data is used
- Personal data and other confidential data should be transferred using encryption and secure password protected devices

Community use of the Internet:

- The school is sensitive to internet related issues experienced by pupils out of school e.g. social networking sites and offers appropriate advice on how to report or deal with inappropriate images, pop-ups or advertisements
- Wider community use of the internet will fall under the same obligations as staff use (refer to the Acceptable Use Agreement)

Introducing the Online Safety Policy to pupils:

- Rules or SMART posters for responsible ICT use are posted around the school as well as in the computing suite
- Pupils are informed that internet use will be monitored
- The Online Safety Committee meet at least once a month to share online safety messages and plan assemblies. They also promote safety online through messages in the weekly newsletter.

Staff and the Online Safety Policy:

- All staff are given the school's Online Safety Policy
- Staff members are made aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential
- An online safety training meeting for staff members is held annually to raise the awareness and importance of safe and responsible Internet use (ICTDS and Flicklearning deliver alternate years)

Enlisting parents' support:

- Parents' attention will be drawn to the school's Online Safety Policy in newsletters, in the prospectus and on the school web site
- Biannual information meetings for parents and pupils are held in school with the online safety coordinator and the Community Police Officer (CPO)

Complaints and Misuse Procedures

It is expected that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse, for example:

.

- Child sexual abuse images
- Adult material which potentially breaches the Obscene Publications Act
- Criminally racist material
- Radicalisation material
- Other criminal conduct, activity or materials

Listed below are the responses that will be made to any apparent or actual incidents of misuse (Also refer to Acceptable Use Agreement, Safeguarding and Child Protection Policies):

- Complaints of internet misuse by pupils will be dealt with by a senior member of staff
- Any complaint about staff misuse must be referred to the Head Teacher immediately
- Complaints of a child protection nature must be reported to the DSL and dealt with in accordance with school child protection procedures
- Any complaint about parent/community misuse of the internet must be referred to the Head teacher immediately
- Any complaint regarding the Head Teacher and misuse of the internet must be referred to the Chair of Governors
- A “Red Whistle Button‟ is available on the VLE for users to report material which could be construed as abusive or inappropriate

Equal Opportunities

All children should have equal access to the use of the internet. Further information on equal opportunities and special needs is given in the relevant school policies.